Travaux pratiques – Utilisation de Wireshark pour examiner les trames Ethernet

Topologie



Objectifs

1re partie : Examiner les champs d'en-tête dans une trame Ethernet II

2e partie : Utiliser Wireshark pour capturer et analyser les trames Ethernet

Contexte/scénario

Lorsque des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI (Open Systems Interconnection) et sont encapsulées dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si les protocoles de couche supérieure sont TCP et IP, et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 sera Ethernet II. C'est généralement le cas pour un environnement de réseau local (LAN).

Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames. Dans la première partie de ces travaux pratiques, vous examinerez les champs figurant dans une trame Ethernet II. Dans la deuxième partie, vous utiliserez Wireshark pour capturer et analyser les champs d'en-tête de trame Ethernet II pour le trafic local et distant.

Ressources requises

• 1 ordinateur (Windows 7, Vista ou XP, doté d'un accès à Internet et sur lequel Wireshark est installé)

1re partie : Examiner les champs d'en-tête dans une trame Ethernet II

Dans la première partie, vous examinerez les champs d'en-tête et le contenu d'une trame Ethernet II. Une capture Wireshark sera utilisée pour examiner le contenu de ces champs.

F4 .							
њт	ano 1 '	IDE ADECTI	ntione at lae	IODAIIDIIRE ADE	champe	a'on_toto	FINDERNOT II
	1 06 .		ULIUII3 EL IE3	IUIIUUEUI 3 UE3	CHAIIDS		
_		 			••••••••••••••••••••••••••••••••••••••		

Préambule	Adresse de Adresse destination source		Type de trame	Données	FCS
8 octets	6 octets	6 octets	2 octets	46-1 500 octets	4 octets

Étape 2 : Examinez la configuration réseau de l'ordinateur.

L'adresse IP de cet ordinateur hôte est 10.20.164.22 et la passerelle par défaut a l'adresse IP 10.20.164.17.

Carte Ethernet Connexion au réseau local : Suffixe DNS propre à la connexion. . . : cisco.com Adresse IPv6 de liaison locale. . . . : fe80::b875:731b:3c7b:c0b1%10 Adresse IPv4. : 10.20.164.22 Masque de sous-réseau. : 255.255.240 Passerelle par défaut. : 10.20.164.17

Étape 3 : Examinez les trames Ethernet dans une capture Wireshark.

La capture Wireshark ci-dessous illustre les paquets générés par une requête ping envoyée depuis un ordinateur hôte à sa passerelle par défaut. Un filtre a été appliqué à Wireshark pour afficher les protocoles ARP et ICMP uniquement. La session commence par une requête ARP pour l'adresse MAC du routeur de passerelle, suivi de quatre requêtes ping et réponses.

	Intel(R)	PRO/10	00 MT N	etwork C	onnection) [Wire:	hark 1.10	0.0 (SVN	Rev 497	90 from /t	trunk-1.10)]											_		×
Eil	e <u>E</u> dit	View	<u>G</u> o <u>C</u>	apture	<u>A</u> nalyze	<u>S</u> tatisti	cs Tele	phony	Tools	Internals	<u>H</u> elp													
0	۲	4	Ø	🖹 🔚	* 2	0	🗢 🔿	4	F 🕹] ⊕,∈) Q	. 🖭	Ù	¥ 🗹	10 %	ġ							
Filt	ter: arp	o or icm	р							▼ Express	ession C	lear	Apply	Sav	/e									
802.	11 Char	nnel:	Chann	el Offset:	FCS	Filter:	All Frame	s	- Non	e .	 Wireless 	Settin	ngs D	ecry	ption k	leys								
No.		Time		Source	1			Destinat	ion		Prote	ocol	Lengt	h	Info									
	7	9.60	117700	0 Dell	_24:2a	:60		Broad	cast		ARP			42	who I	nas 10.	20.164.	17?	Tell 10). 20	0.164.	22		
	8	9.60	180300	0 Cisc	o_7a:eo	::84		De11_	24:2a:	60	ARP			60	10.20	0.164.1	7 is at	30:	F7:0d:7a	:ec	c:84			
	9	9.60	182700	0 10.2	0.164.2	22		10.20	.164.1	.7	ICM	P		74	Echo	(ping)	reques	t i	d=0x0001	., s	seq=37	/9472,	tt]=1	L28
	10	9.60	280700	0 10.2	0.164.1	L7		10.20	.164.2	2	ICM	Р		74	Echo	(ping)	reply	i	d=0x0001	., s	seq=37	/9472,	tt]=	255
	12	10.6	041870	0(10.2)	0.164.2	22		10.20	.164.1	.7	ICM	P		74	Echo	(ping)	reques	t i	d=0x0001	., s	seq=38	/9728,	tt]=1	L28
	13	10.6	207280	0(10.2)	0.164.1	L7		10.20	.164.2	2	ICM	Р		74	Echo	(ping)	reply	i	d=0x0001	., s	seq=38	/9728,	tt]=	255
	14	11.6	071920	0(10.2)	0.164.2	22		10.20	.164.1	.7	ICM	Р		74	Echo	(ping)	reques	t i	d=0x0001	., s	5eq=39	/9984,	ttl=1	L28
	15	11.6	081770	0(10.2)	0.164.1	L7		10.20	.164.2	2	ICM	P		74	Echo	(ping)	reply	i	d=0x0001	., s	seq=39	/9984,	ttl=2	255
	17	12.6	102580	0(10.2)	0.164.2	22		10.20	.164.1	.7	ICM	Р		74	Echo	(ping)	reques	t i	d=0x0001	., s	seq=40	/10240	, ttl⊧	=128
	18	12.6	113180	0(10.2)	0.164.1	L7		10.20	.164.2	2	ICM	P		74	Echo	(ping)	reply	i	d=0x0001	., s	seq=40	/10240	, ttl:	=255
٠.									III									_						Þ
+	Frame	7:4	2 byte	s on w	ire (3	36 bi1	s), 4	2 byte	s cap	tured ((336 bit	s) o	on int	ert	face	0								
	Etheri	net I	I, Src	: Dell	_24:2a	:60 (c:26:	0a:24:	2a:60), Dst:	: Broadc	ast	(ff:f	f:t	ff:ff	:ff:ff)	1							
	E Dest	tinat	ion: B	roadca	st (ff	:ff:ff	f:ff:f	f:ff)																
	E Sou	rce:	De11_2	4:2a:6	0 (5c:	26:0a	24:2a	:60)																
	тур	e: AR	P (0x0	806)																				
± ,	Addre	ss Re	soluti	on Pro	tocol	(reque	est)																	
000	0.14				5 - 26		2- 60		c 00 0			¢												
000		00 (0) 00 (0)	06 04 0 00 00 0	DO 01	oc 26 5c 26 0a 14	0a 24 0a 24 a4 11	2a 60 2a 60) 08 0) 0a 1	6 00 0 4 a4 1	16 	\& \&	\$*`. \$*`.												

Étape 4 : Examinez le contenu d'en-tête Ethernet II d'une requête ARP.

Le tableau suivant prend la première trame dans la capture Wireshark et affiche les données dans les champs d'en-tête Ethernet II.

Champ	Valeur	Description						
Préambule	Non affichée dans la capture.	Ce champ contient des bits de synchronisation traités par la carte réseau.						
Adresse de destination	Broadcast (ff:ff:ff:ff:ff)	Les adresses de couche 2 pour la trame. Chaque adresse fait 48 bits de long, ou 6 octets, exprimés sous la forme de						
Adresse source	Dell_24:2a:60	12 cniffres nexadecimaux , 0-9, A-F. Un format courant est 12:34:56:78:9A:BC.						
	(30.20.08.24.28.00)	Les six premiers chiffres hexadécimaux indiquent le fabricant de la carte réseau, les six derniers chiffres hexadécimaux correspondent au numéro de série de la carte réseau.						
		L'adresse de destination peut être une adresse de diffusion, qui ne contient que des 1, ou une adresse à monodiffusion. L'adresse source est toujours à monodiffusion.						
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet II. Deux types de trame standard sont :						
		Valeur Description						
		0x0800 Protocole IPv4 0x0806 Protocole ARP (Address Resolution Protocol)						
Données ARP		Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1 500 octets.						
FCS	Non affichée dans la capture.	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par l'ordinateur émetteur, et englobe les adresses de trames, le type et le champ de données. Elle est vérifiée par le récepteur.						

Quel élément est-il important en ce qui concerne le contenu du champ d'adresse de destination ?

Pourquoi l'ordinateur envoie-t-il une diffusion ARP avant d'envoyer la première requête ping ?

Quelle est l'adresse MAC de la source dans la première trame ?

Quel est l'ID du fournisseur (OUI) de la carte réseau source ?

À quelle partie de l'adresse MAC correspond l'identifiant OUI ?

Quel est le numéro de série de la carte réseau source ?

2e partie : Utiliser Wireshark pour capturer et analyser les trames Ethernet

Dans la deuxième partie, vous utiliserez Wireshark pour capturer les trames Ethernet locales et distantes. Vous examinerez ensuite les informations contenues dans les champs d'en-tête de trame.

Étape 1 : Déterminez l'adresse IP de la passerelle par défaut sur votre ordinateur.

Ouvrez une fenêtre d'invite de commandes et entrez la commande ipconfig.

Quelle est l'adresse IP de la passerelle par défaut de l'ordinateur ?

Étape 2 : Commencez par capturer le trafic sur la carte réseau de votre ordinateur.

- a. Ouvrez Wireshark.
- b. Dans la barre d'outils de l'outil d'analyse de réseaux Wireshark, cliquez sur l'icône Interface List (Liste d'interfaces).



c. Dans la fenêtre Wireshark: Capture Interfaces (Wireshark : interfaces de capture), sélectionnez l'interface pour commencer la capture du trafic en activant la case à cocher appropriée, puis cliquez sur Démarrer. Si vous n'êtes pas sûr de l'interface à vérifier, cliquez sur Details pour plus d'informations sur chaque interface répertoriée.

1	Wireshark: Capture Interfaces			• ×
	Description IP	Packets	Packets/s	
	🔲 🛃 Sun fe80::50e4:c3e6:b635:a999	26	0	Details
	🕡 🖅 Intel(R) 82577LM Gigabit Network Connection fe80::b875:731b:3c7b:c0b1	95	1	<u>D</u> etails
(Help Start Stop	Option:	5	<u>C</u> lose

d. Observez le trafic qui apparaît dans la fenêtre Packet List (Liste de paquets).

_				
Fil	lter:	 Expression. 	Clear /	Apply Save
802	.11 Channel: 💌 Channel Offset: 💌 FCS Filter: All Frame	s 💌 None 💌 Wi	reless Settin	ngs Decryption Keys
No.	Time Source	Destination	Protocol	Lenath Info
	18 10.40268/00(184.2/.190.41	10.20.104.22	TCP	60 NTTPS > 62408 [ACK] SEQ=1 ACK=1163 W1N=43412 LEN=0
	19 10.60449100(184.27.190.41	10.20.164.22	TLSV1	587 Application Data
	20 10.80121900(10.20.164.22	184.27.190.41	TCP	54 62408 > https [ACK] seq=1163 Ack=534 Win=16695 Len=0
	21 11.04927800(10.20.164.22	10.20.164.31	NBNS	92 Name query NB HP094B61<00>
	22 11.79926500(10.20.164.22	10.20.164.31	NBNS	92 Name query NB HP094B61<00>
	23 12.03732100(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
	24 12.06936200(10.20.164.22	192.168.87.9	SNMP	120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.
	25 14.03733500(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
	26 16.03704300(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
	27 18.03657200(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
	28 19.75046200(10.20.164.22	70.42.228.171	TCP	66 62423 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1
	29 19.81045200(70.42.228.171	10.20.164.22	TCP	66 https > 62423 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1260 SACK_PERM=1 w
	30 19.81054600(10.20.164.22	70.42.228.171	тср	54 62423 > https [ACK] Seq=1 Ack=1 win=66780 Len=0

Étape 3 : Filtrez Wireshark pour afficher uniquement le trafic ICMP.

Vous pouvez utiliser le filtre dans Wireshark pour bloquer la visibilité du trafic indésirable. Le filtre ne bloque pas la capture des données indésirables ; il filtre uniquement ce qui doit s'afficher à l'écran. Pour le moment, seul le trafic ICMP doit être affiché.

Dans la zone Filter (Filtre) de Wireshark, saisissez icmp. La case devient verte si vous avez tapé le filtre correctement. Si la case est verte, cliquez sur Appliquer (Apply) pour appliquer le filtre.

Filter:	icmp	•	Expression	Clear	Apply	Save	
---------	------	---	------------	-------	-------	------	--

Étape 4 : À partir de la fenêtre d'invite de commandes, envoyez une requête ping à la passerelle par défaut de votre ordinateur.

À partir de la fenêtre de commandes, envoyez une requête ping à la passerelle par défaut avec l'adresse IP que vous avez enregistrée à l'étape 1.

Étape 5 : Arrêtez la capture du trafic sur la carte réseau.

Cliquez sur l'icône Stop Capture (Arrêter la capture) pour arrêter la capture du trafic.



Étape 6 : Examinez la première requête Echo (ping) dans Wireshark.

La fenêtre principale de Wireshark est divisée en trois sections : le volet Packet List (Liste des paquets) (en haut), le volet Packet Details (Détails des paquets) (au milieu) et le volet Packet Bytes (Octets des paquets) (en bas). Si vous avez sélectionné l'interface appropriée pour la capture des paquets à l'étape 3, Wireshark doit afficher les informations ICMP dans le volet Packet List (Liste des paquets) de Wireshark, comme dans l'exemple suivant.

Intel(R) 82577LM Gigabit Network Connection: \Device	:e\NPF_{6179E093-A447-4EC8-81DF-5	E22D08A6F63} [Wireshark 1.8.3	(SVN Rev 45256 from /	trunk-1.8)]
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> e	elp		
	. 🔅 🔿 🗛 🕹 🔲 🗐		M 🖪 💥 🕅	
Filter: icmp	 Expressio 	n Clear Apply Save		
802.11 Channel: Channel Offset: FCS Filter: All	Frames Vone V	Vireless Settings Decryption K	(eys	
No. Time Source	Destination	Protocol Length Info		
9 9.601827000 10.20.164.22	10.20.164.17	ICMP 74 Echo	(ping) request	id=0x0001, seq=37/9472, ttl=128
10 9.602807000 10.20.164.17	10.20.164.22	ICMP 74 Echo	(ping) reply	id=0x0001, seq=37/9472, tt1=255
12 10.60418/00(10.20.164.22	10.20.164.17	ICMP /4 Echo	(ping) request	1d=0x0001, seq=38/9/28, tt1=128
13 10.620/2800(10.20.164.1/	10.20.164.22	ICMP /4 ECHO	(ping) reply	1d=0x0001, seq=38/9/28, tt1=255
15 11 60817700(10.20.164.17	10.20.164.17	TCMP 74 ECHO	(ping) request	id=0x0001, Seq=39/9984, tt1=128
17 12 61025800(10 20 164 22	10.20.164.17	TCMP 74 ECHO	(ping) request	id=0x0001, Seq=39/9984, CU1=233
18 12 61131800(10 20 164 17	10.20.164.22	TCMP 74 Echo	(ping) reply	id=0x0001, seq=40/10240, tt1=255
10 12:01191000(10:20:104:1/	10.20.104.22	1011 74 2010	(ping) reply	14-0x0001, 304-40/10240, 001-235
•				4
Ename Or 74 butter on wine (502 bits) 74 but of conturned (EO)) hits) on intenface (0	
Frame 9: 74 bytes on wire (392 bits	(392), 74 bytes captured (392)	isco 72:00:84 (20:f7:	0 0d:70:00:84)	
Thernet Protocol Version 4 Src: 1	0 20 164 22 (10 20 164 22	2) Det: 10 20 164 17	(10 20 164 17)	
Thternet Control Message Protocol	0.20.104.22 (10.20.104.22	2), 030. 10.20.104.17	(10.20.104.17)	
Internet control Message Prococor	Milie	u		
0000 30 f7 0d 7a ec 84 5c 26 0a 24 2	2a 60 08 00 45 00 0z.	.\& .\$*`E.		
0020 a4 11 08 00 4d 36 00 01 00 25 6	51 62 63 64 65 66	16. %abcdef		
0030 67 68 69 6a 6b 6c 6d 6e 6f 70	71 72 73 74 75 76 ghijk	lmn opqrstuv		
0040 77 61 62 63 64 65 66 67 68 69	wabcd	lefg hi		
	Rac			
	Dus			

a. Dans le volet Packet List (Liste des paquets) (section supérieure), cliquez sur la première trame répertoriée. Echo (ping) request devrait s'afficher en dessous de l'en-tête Info. La ligne devrait également être mise en surbrillance en bleu.

- b. Examinez la première ligne du volet Packet Details (Détails des paquets) (section centrale). Cette ligne indique la longueur de la trame : 74 octets dans cet exemple.
- c. La deuxième ligne dans le volet Packet Details (Détails des paquets) indique qu'il s'agit d'une trame Ethernet II. Les adresses MAC source et de destination sont également indiquées.

Quelle est l'adresse MAC de la carte réseau de l'ordinateur ?

Quelle est l'adresse MAC de la passerelle par défaut ?

d. Vous pouvez cliquer sur le signe plus (+) au début de la seconde ligne d'obtenir des informations supplémentaires sur la trame Ethernet II. Notez que le signe plus devient un signe moins (-).

Quel type de trame est affichée ?

e. Les deux dernières lignes figurant dans la section centrale fournissent des informations sur le champ de données de la trame. Notez que les données contiennent les informations d'adresse IPv4 de la source et de la destination.

Quelle est l'adresse IP source ?

Quelle est l'adresse IP de destination ?

f. Vous pouvez cliquer sur n'importe quelle ligne dans la section centrale pour mettre en surbrillance cette partie de la trame (hex et ASCII) dans le volet Packet Bytes (Octets des paquets) (section inférieure). Cliquez sur la ligne **Internet Control Message Protocol** dans la section centrale et examinez ce qui est mis en surbrillance dans le volet Packet Bytes (Octets des paquets).

🕢 Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0	
Hethernet II, Src: Dell_24:2a:60 (5c:26:0a:24:2a:60), Dst: Cisco_7a:ec:84 (30:f7:0d:7a:ec:84)	
HINTER INTERNET PROTOCO Version 4, Src: 10.20.164.22 (10.20.164.22), Dst: 10.20.164.17 (10.20.164.17)	E
Internet Control Message Protocol	
Type: 8 (Echo (ping) request)	
Code: 0	
Checksum: 0x4d4e [correct]	Ŧ
0000 30 f7 0d 7a ec 84 5c 26 0a 24 2a 60 08 00 45 00 0.z\& .5*`.E. 0010 00 3c 03 48 00 00 80 01 db 29 0a 14 a4 16 0a 14	

Quelles sont les deux dernières lettres des octets mis en surbrillance ?

g. Cliquez sur la trame suivante dans la section supérieure et examinez une trame de réponse Echo. Notez que les adresses MAC source et de destination ont été inversées, car cette trame a été envoyée depuis le routeur de passerelle par défaut comme réponse au premier ping.

Quel périphérique et quelle adresse MAC s'affichent-ils comme adresse de destination ?

Étape 7 : Redémarrez la capture de paquets dans Wireshark.

Cliquez sur l'icône **Start Capture (Démarrer la capture)** pour démarrer une nouvelle capture Wireshark. Une fenêtre contextuelle vous invite à enregistrer les précédents paquets capturésdans un fichier avant de démarrer une nouvelle capture. Cliquez sur **Continue without Saving (Continuer sans enregistrer)**.



Étape 8 : Dans la fenêtre d'invite de commandes, envoyez une requête ping à www.cisco.com.

Étape 9 : Arrêtez la capture des paquets.

🙍 Capturing from Intel(R) 82577LM Gigabit												
<u>F</u> ile	<u>F</u> ile <u>E</u> dit		<u>G</u> o	<u>C</u> aptu	<u>A</u> nalyz							
0	•		0			×	1					

Étape 10 : Examinez les nouvelles données dans le volet de la liste des paquets de Wireshark.

Dans la première trame de demande Echo (ping), quelles sont les adresses MAC source et de destination ?

Source : _____

Destination : _____

Quelles sont les adresses IP source et de destination figurant dans le champ de données de la trame ?

Source : _____

Destination :

Comparez ces adresses aux adresses que vous avez reçues à l'étape 7. La seule adresse qui a changé est l'adresse IP de destination. Pourquoi l'adresse IP de destination a-t-elle changé, alors que l'adresse MAC de destination est resté la même ?

Remarques générales

Wireshark n'affiche pas le champ de préambule d'un en-tête de trame. Que contient le champ de préambule ?